SIM　BLE　認証

Technology Reports

新しいサービス創出に向けたポータブルSIMの開発

スマートフォンの浸透により，その利便性を高めるためのサービス開発が急速に進んできている．また，ポストスマートフォンを見据えたデバイスや，それを活用するシステムやサービスの開発も加速している．今回，ポストスマートフォンに向けた新しいデバイスとして，認証機能を携帯電話から切り出したポータブルSIMという新しい小型認証デバイスを開発した．本稿では，ポータブルSIMの基本構成，基本動作について解説するとともに，ポータブルSIMが作り出す新たな世界についても述べる．

移動機開発部　渋谷 彰　名知 数馬
樋口 雄太　岡田 隆

1. まえがき

スマートフォンの浸透が急速に進み，早くも現在のスマートフォンの次（ポストスマートフォン）を狙う動きが加速している．その中で，腕時計型，メガネ型，健康関連機器などのウェアラブルデバイスが発売され，スマートフォンと連携させる利用形態の提案が行われている．この傾向が進むと，ウェアラブルを含め，一人で複数台の機器を所有するマルチデバイスの時代になるものと考えられる．

さらに近年，センサ，スマートメータ，自動車，冷蔵庫などのあらゆるものがインターネットに接続するIoT（Internet of Things）の概念が提案[1]され，各方面で開発が進められている．これが浸透してくると，多様な通信デバイスが爆発的に増加していくものと考えられる．

また一方，SNS，ショッピング，電子決済，コンテンツ視聴などのモバイルITサービスもスマートフォンの浸透と同じように進んでいる．これらのサービスでは，ユーザを特定する手段としてIDとパスワードが最も簡易な手段として使われている．しかしながら，漏えいした際のリスクが高い決済情報が扱われるようになったことや，サービスの多様化に伴いユーザが管理するID数が多くなったことにより，よりセキュアでかつ簡易なID管理方法が要望されている．

このような背景の中で，ポストスマートフォンの概念について検討を実施した．その結果，これまでの携帯電話の進化は，ユーザにさまざまなサービスを使ってもらうため，機能を順次追加してAll in Oneを追求する形で進化してきたが，今後は，端末形態に関係なく（マルチデバイス環境下で）ユーザが多様なサービスに接続できることが重要であるとの結論に至った．

この結論から，現状のスマートフォンの機能を見直すと，ポストスマートフォンのコアな機能としてUI，セルラネットワークへのアクセス機能は常時必要とされるものではなく，ユーザ認証に必要なSIM（Subscriber Identity Module）*1のみを所持し，必要なときに必要なデバイスを有効化し利用できれば十分である．これは，認証デバイスであるSIMをコアとした小型デバイスを構成できればよいことを意味している．

*1 SIM：携帯電話の契約情報を記録したICカード．

今回開発した「ポータブルSIM」は上記の発想に基づき，SIMを端末から切り離し小型デバイスとして構築したものである（**図1**）．本稿では，今回開発したポータブルSIMのハードウェア構成およびスマートフォン側のソフトウェア構成を示し，併せて，ポータブルSIMの基本動作を解説する．最後に，ポータブルSIMにより創出される新しい世界を紹介する．

2. ポータブルSIMの構成

今回開発したポータブルSIMの試作機の外観を**写真1**に，主要諸元を**表1**に示す．

ポータブルSIMを構成するにあたり，SIM自体は通信する機能を有していないので，通信機能を搭載する必要がある．また，携帯電話から切り出して小型機器として成り立たせるためには，低消費電力である必要がある．さらに，さまざまな通信機器との接続の容易性も考慮する必要がある．この観点から，ポータブルSIMと通信機器の接続方法には，スマートフォンに標準的に搭載され，

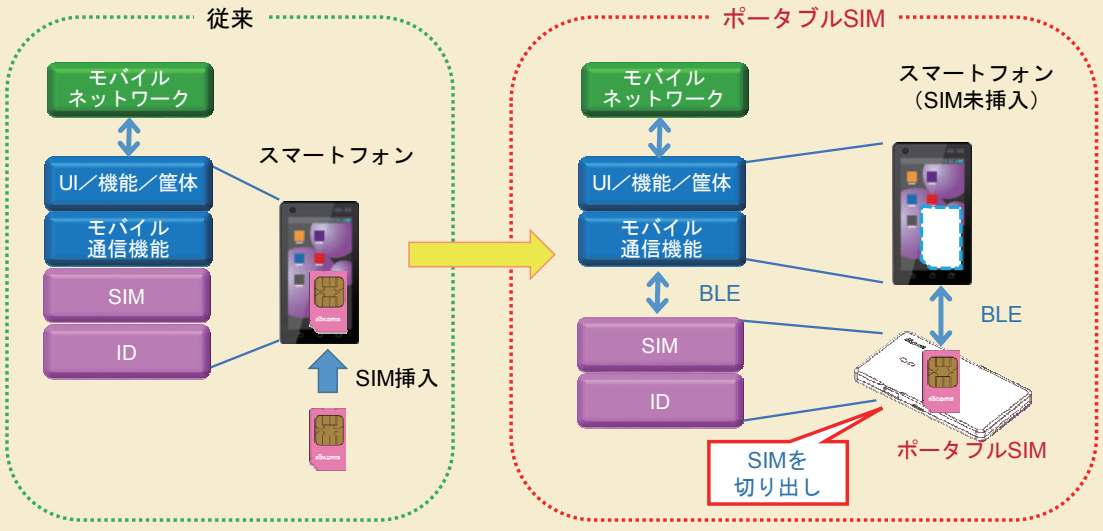

図1　ポータブルSIMのコンセプト

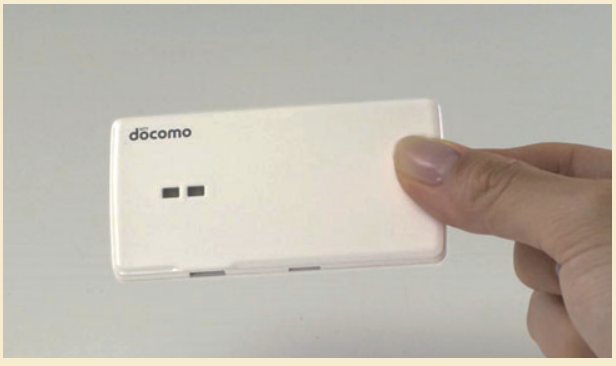

写真1　ポータブルSIM試作機の外観

かつPCなどのさまざまな機器にも普及が進んでいるBluetooth®[*2]，中でも低消費電力化が実現可能なBluetooth Ver4.0（通称BLE：Bluetooth Low Energy）を採用した．また，ID管理およびBLE接続時の利便性の向上の観点からNFC（Near Field Communication）[*3]も搭載している（**図2**）．

SIMを外部機器と接続する場合，情報をセキュアに受け渡すために信頼性の高いプロトコルを用いる必要がある．Bluetoothにおいては，この要求を満たすプロトコルとして従来からSAP（SIM Access Profile）が存在している[2]．しかしながら，BluetoothとBLEの規格の違いからSAPをBLEにそのまま適用できない．そこで，SAPのポリシーに従い，BLE上で動作する新たなプロファイル[*4]（SAP on BLE）を開発した．

SAP on BLEは，BLE上にSAPを構築したものである．ここでは，まず，BluetoothのコマンドをBLEのコマンドと1対1となるように再定義した．さらに，BLEでは，Clientから処理要求送信後，Serverにて処理完了後にレスポンスを送信するという動作が行えないため，BLE上のコマンドを割り当てることでレスポンス処理を実現させた．また，SAPでは，暗号方式として3DES（Triple Data Encryption Standard）を利用しているが，SAP on BLEではBLE上で定義されているAES（Advanced Encryption Standard）[*5]による暗号化通信を実現している．

ポータブルSIMに対応させるための携帯電話側のソフトウェア構成を**図3**に示す．携帯電話側では，BLEを経由してモデム（Modem）にSIM情報が受け渡せるようにする必要がある．また，携帯電話内での他のアプリケーションからのセキュリティ確保や，今後のサービス創出に向けた機能追加の容易性にも配慮する必要がある．このような観点から，SAP on BLEの携帯電話側ソフトウェア（Application for Portable SIM）はJava Layerに配置し，Native Layerに配置しているDaemonソフト（Daemon for Modem Comm.）を介してモデムと接続する構成とした．

このようなソフトウェア構成を用いることにより，モデムとOSに依存する部分はDaemonソフトで吸収できるため，SAP on BLEに大幅な変更を加えることなくさまざまな通信機器への対応も容易になる．なお，SAP on BLEで，ポータブルSIM側をPeripheral[*6]，携帯電話側をCentral[*7]として実装することで携帯電話からSIMの切り出し，外部からの接続を実現した．

3. ポータブルSIMの基本動作

スマートフォンなどの通信機器において，ポータブルSIMを用いてサービスを利用する際の基本動作は以下のとおりである（**図4**）．

①BLEリンクの確立

ポータブルSIMと通信機器間でBLEリンクに必要な情報を交換する．その情報に基づき，ポータブルSIMと通信機器間でBLEリンクを確立する．

本試作では，BLEリンク確立に必要な情報の交換には，NFC通信を用いており，「タッチ」という簡易，かつ直感的な操作で接続できる方法を実装し

表1　ポータブルSIM試作機の主要諸元

寸　法 （高さ×幅×厚さ：mm）	約80×40×5.6
質　量	約20g
通信方式	NFC/Bluetooth（4.0）
給電方式	USB充電

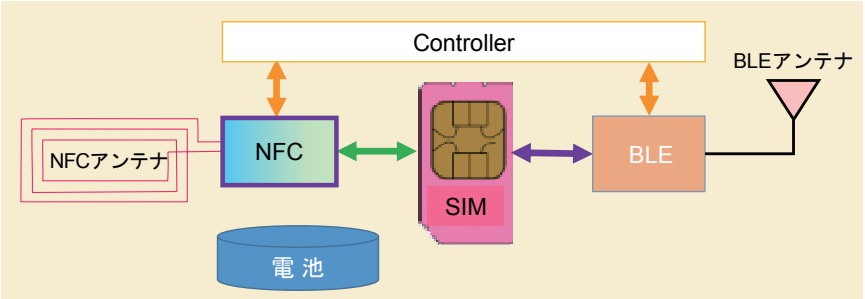

図2　ポータブルSIMのハードウェア構成

＊2 **Bluetooth®**：移動端末，ノートPCなどの携帯端末を無線により接続する短距離無線通信規格で，米国Bluetooth SIG Inc.の登録商標．

＊3 **NFC**：NXPセミコンダクターズ社とソニーが開始した13.56MHz帯の近距離無線通信規格で，FeliCa®やMifare®およびType A/B（ISO14443），ICタグ（ISO/IEC 15693）を統一してサポートしている．

＊4 **プロファイル**：BluetoothやBluetooth Low Energyで通信する際に使用される，サービスごとに策定された機器間のプロトコル．

＊5 **AES**：アメリカ合衆国の新暗号規格として規格化された共通鍵暗号方式であり，3GPPでも利用される暗号方式の1つ．

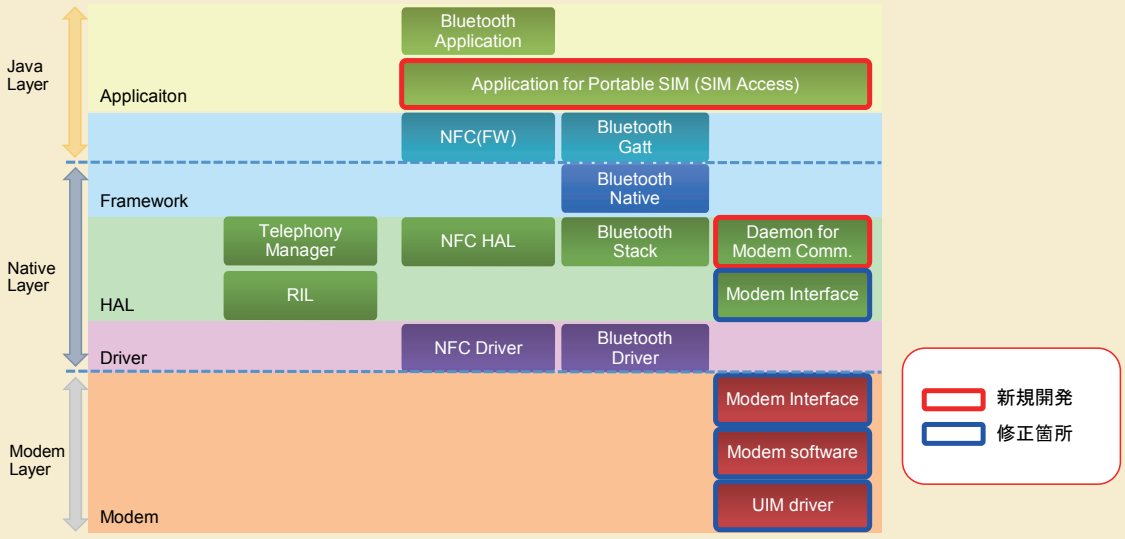

図3　ポータブルSIM対応スマートフォンのソフトウェア構成

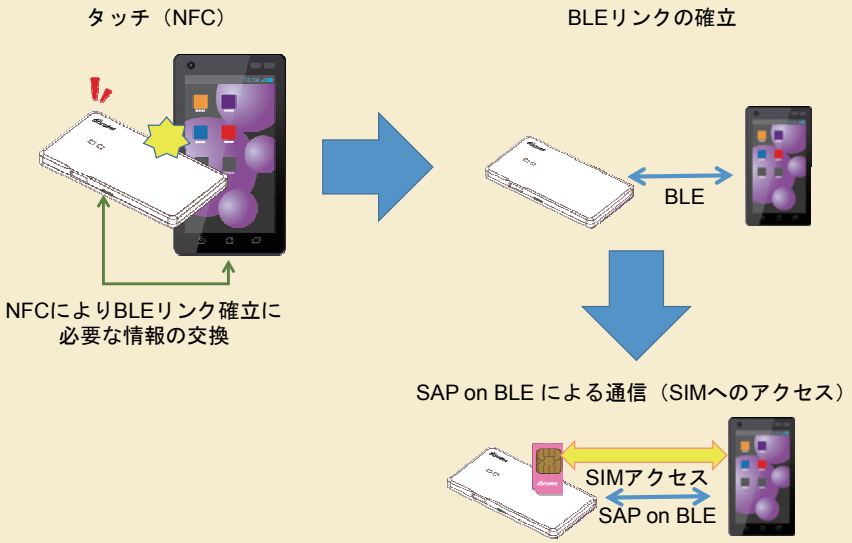

図4　ポータブルSIMの利用イメージ

ている．

②SAP on BLEによる通信

BLEリンクが確立された後，前述のSAP on BLEプロファイルを用いてSIMと通信機器を接続する．この時，通信機器がモバイルネットワーク接続に必要な情報は，通信機器のモデムからの指示に応じてポータブルSIMが通信機器へ送出する．通信機器側では，SIMが内蔵されている際と同じ処理が実施される．

③SE領域の利用

SIMのSE（Secure Element）[*8]に格納されている情報は，NFCタッチにより送出される．BLEリンクが確立されている場合には，SAP on BLEプロファイル

＊6 **Peripheral**：Bluetooth Low Energyにおける機器の役割．Central（＊7参照）とPeripheralに区別され，CentralがPeripheralの検出や制御を行う．

＊7 **Central**：Bluetooth Low Energyにおける機器の役割．CentralとPeripheralに区別され，CentralがPeripheralの検出や制御を行う．

＊8 **SE**：暗号化鍵や秘匿情報などをセキュアに格納する領域．

を用いても送出可能である．

これらのポータブルSIMの基本動作を組み合わせることで，マルチデバイス利用時，デバイスシェアリング時，およびID認証時のユーザ利便性が向上する．以下で3つの利用シーンについて説明する（**図5**）．

・マルチデバイス

タブレットにポータブルSIMを接続することで，携帯電話の各種機能がポータブルSIMの携帯電話番号で利用可能となる．その後，同じポータブルSIMをスマートフォンに接続すると，タブレットで利用していた各種機能が同じ番号で利用できるようになる．この時，タブレットは利用不可となる．

家では，画面の大きなタブレットを使用し，移動中は持ち運びやすいスマートフォンといった利用方法が可能となる．

・デバイスシェアリング

1つの通信機器に対してポータブルSIMを複数台持ち，接続を切り替えるだけでユースケースに応じた使い分けが簡単にできる．

例えば，プライベート用ポータブルSIMとビジネス用ポータブルSIMというように，2つのポータブルSIMを持ち，1つのスマートフォンをプライベートと仕事で使い分けることができる．また，家族で1台のタブレットを共用するようなケースでも，家族それぞれのポータブルSIMを利用し，ユーザに合わせた設定で利用することが可能となる．

つまり，電話番号と連携してMDM（Mobile Device Management）機能を使うと，例えば，ビジネス用ポータブルSIM利用時のカメラやアプリの起動抑止設定，もしくは，家族共用タブレットでは，子どものポータブルSIM利用時のパレンタルコントロール*9も可能である．

・ID認証

SIMカードのSE領域に普段利用しているサービス認証情報（Webアドレス，ID・パスワードなど）を格納しておくことで，マルチデバイス利用時，IoTデバイス使用時など，さまざまな通信機器を渡り歩いても，同じサービス認証情報を簡単に利用できる．

4. ポータブルSIMにより拡がる世界

ポータブルSIMにより，電話番号や設定の切替え，サービス認証情報の持運びが簡単に行えるようになり，

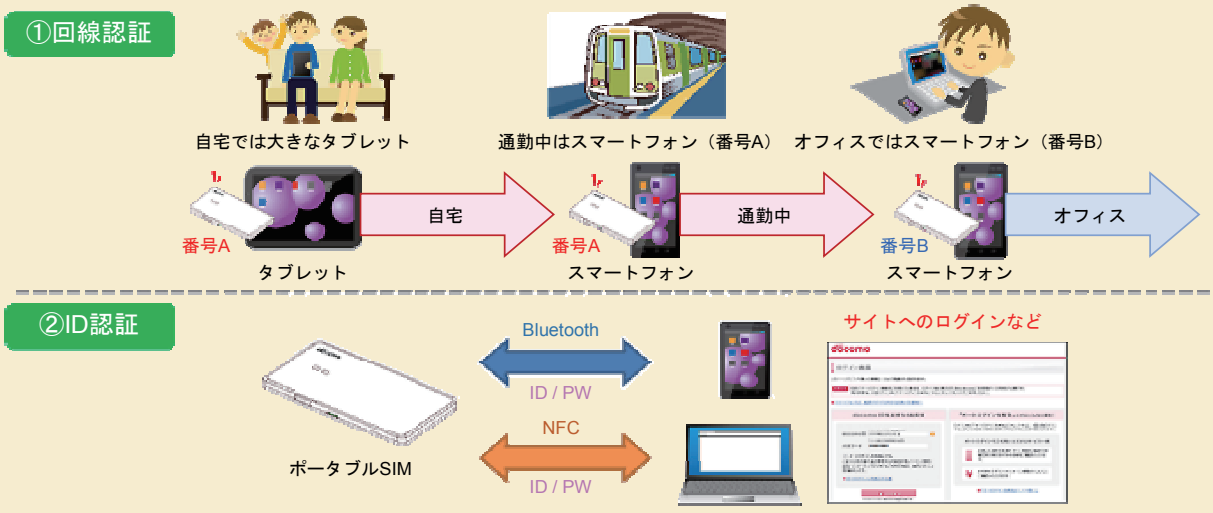

図5　ポータブルSIMの利用シーン

＊9　**パレンタルコントロール**：子どもによるスマートフォンやパソコンなどのデバイス利用を，親が制限可能な機能．

電話番号やサービス認証情報を持ち歩く環境を作り上げることができる．これにより創出される新しい世界を以下で説明する（**図6**）．

⑴モノと人の組合せを柔軟に変えられる世界の創造

ポータブルSIMが提供する直接的な価値は「自分の電話番号（利用者の特定）／IDの持ち運び」である．一方，今後展開が進むと予測されているIoTの世界では，利用者がモノ（スマートフォンなどの通信機能を有するデバイスなど）を通じてネット（インターネットやセルラーネット）につながる際，サービスを提供する上で利用者の特定がきわめて重要となる．このIoTの世界でポータブルSIMの価値を考えると，モノ側の観点では「モノと回線（契約）の分離」により，回線（契約）を気にすることなくあらゆるモノを容易にネットの入口にするという利点を提供できる．これと同時に，利用者側の観点ではいたる所に存在するネットの入口から所望のサービスへ容易に到達するという利点を提供できる．つまり，ポータブルSIMを用いれば，**図7**のように，サービス利用者の特定が容易になるため，従来のようにモノと回線契約・利用者（人）が固定した世界ではなく，利用するモノを所有せずにモノと利用者（人）の組合せを柔軟に変えられる世界を作り上げることが可能となる．これが，“所有から利用へ”といった新たな価値創出につながると考える．

例えば，健康サービスを利用している利用者は，利用者の周辺にある健康機器を初めて利用する場合であっても，ポータブルSIMによる直感的な操作で，健康機器で取得されたデータとともに利用者を健康サービスまで導くことが可能となる．また，自動車を利用する際にも，乗車時に容易に利用者を特定することができ，クラウド上で作成した旅行計画（経由地，お気に入りの場所など）をカーナビに設定したり，またお気に入りの音楽再生など車載機器と連携し，利用者に応じたサービスをシームレスに提供することが可能となる．

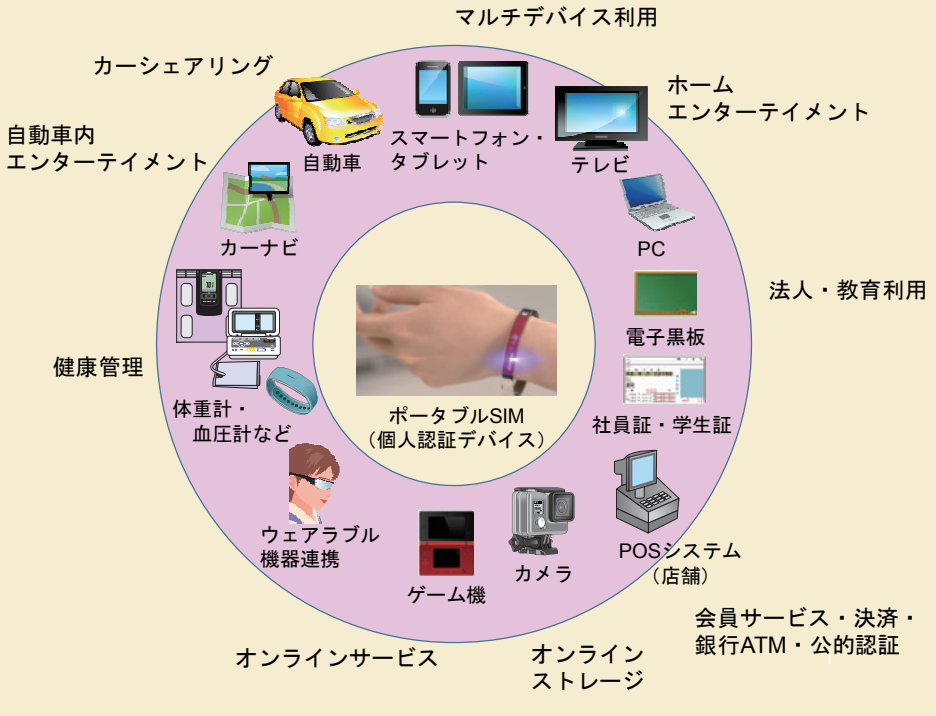

図6　ポータブルSIMにより拡がる世界

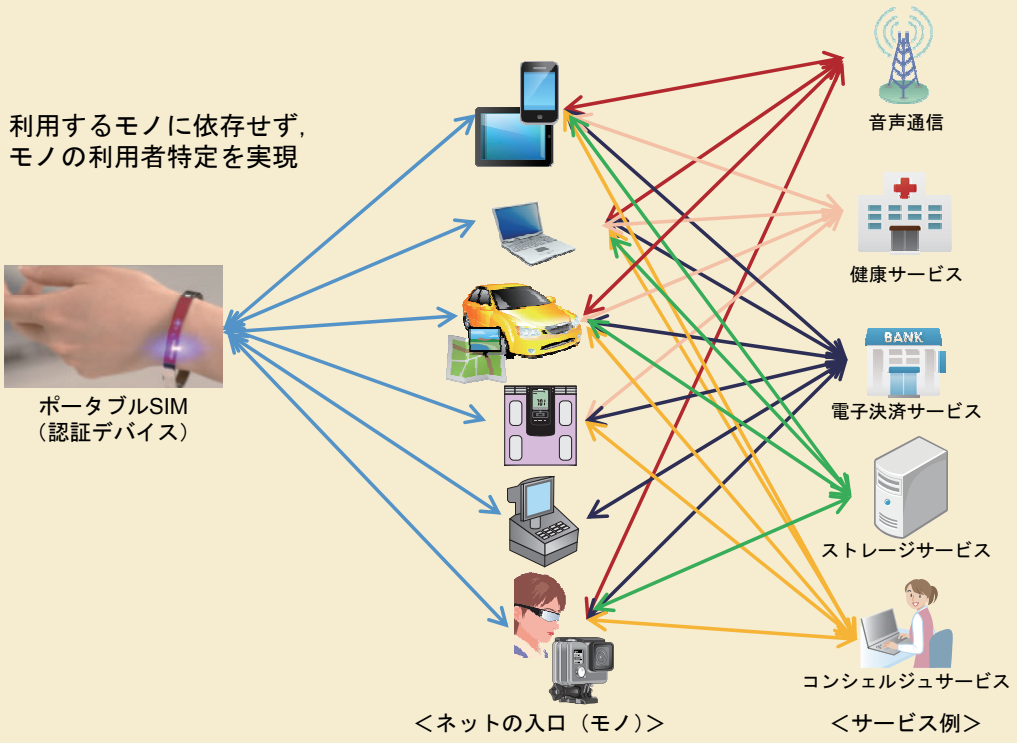

図7　モノと利用者の柔軟な組合せ

⑵セキュアでオープンな認証機能の提供

これまでSIMはスマートフォンに内蔵して利用されていたが，ポータブルSIMという新たな機能デバイスを構築することで，従来からSIMに具備されている機能をポータブルSIM単独で利用することができる．これがポータブルSIMの直接的な価値の2つ目である．具体的なイメージを**図8**に示す．

SIMには，紛失時の対応として，PIN認証や紛失時の遠隔停止[4]機能も有しており，ポータブルSIM紛失時でも遠隔停止により認証機能を無効化することが可能である．加えて，TSM（Trusted Service Manager）と呼ばれるサービス発行管理システム[3]から，SEにアプレット*10 [4]をアドオンできる仕組みが搭載されている．ここで，SEに格納するアプレットは，Java Card™*11 [4]によるプログラム開発が可能であり，ID/PW管理機能や，会員証，電子錠，住基カード認証機能などの認証機能が容易に追加できる．つまり，ポータブルSIMに格納したアプレットを用いて，様々なサービスと接続するための個人認証を行うことが可能である．

これにより，サービス提供者の観点では，これまで個人認証用に配布していたカードなどのデバイスを用いることなく，サービスに応じた独自の認証基盤を構築することができるという利点が生まれる．また同時に，利用者の観点では，安全性を担保しつつサービスごとに分散していた認証機能の集約が図れ，ID/PW管理の煩雑さから解放されるという利点が生まれる．さらに，これらを総合して，セキュアな認証基盤を必要とするサービス間でも連携を強められることから，新しいサービス創出につながると考える．

たとえば，回線認証と組み合わせることでポータブルSIM上のアプレット管理（追加／削除など）を自動化し，個々の認証機能が保持しているパスワードや署名情報などの更新を利用者の手間をかけずに実施できるようになる．また，認証機能が集約されることで異なるサービス事業者間でコンテンツ決済機能の連携

＊10 アプレット：SIM上で動作するJavaCard™（＊11参照）アプリケーション．

＊11 Java Card™：SIMを含むスマートカードなどの限られたメモリと処理能力しかないデバイス上で実行するJava実行環境．Javaは，Oracle Corporationおよびその子会社，関連会社の米国およびその他の国における登録商標．

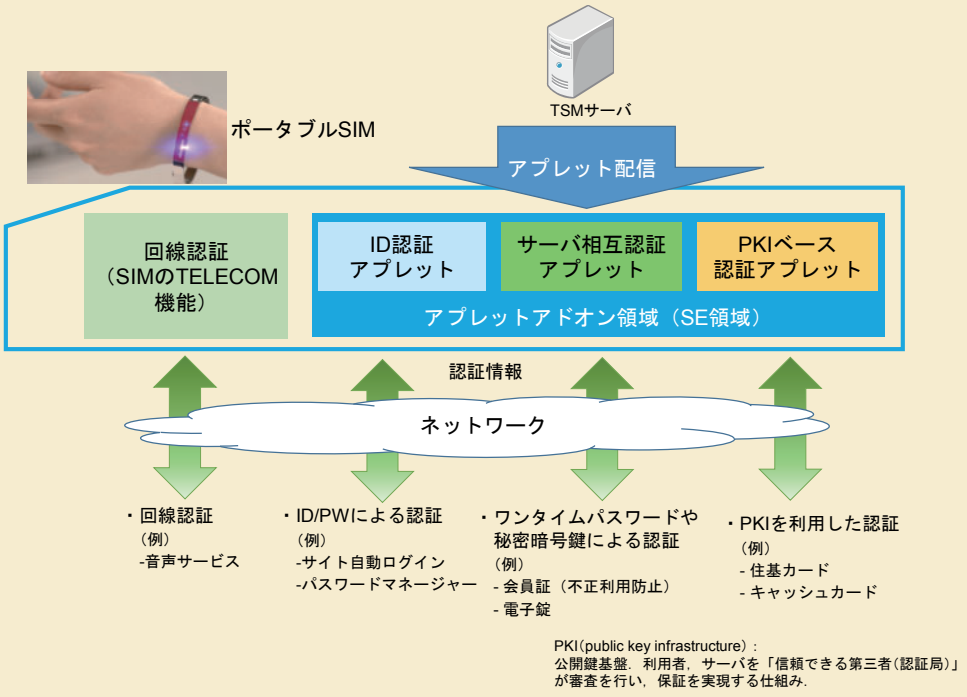

図8　ポータブルSIMを活用した認証

が容易となり，ポイントや特典の相互利用も容易に実現できるようになると考えられる．さらに，健康・医療の分野では，病院間でのカルテなどの高セキュアに管理される個人情報の連携も図れ，利便性の向上につながるものと考えられる．

このように，ポータブルSIMでは，ネットの入口を増やし，人とモノとサービスの組合せを柔軟に変えられ，かつ，サービスの種類に応じたさまざまな認証機能を実現できる．これらを1つに統合することで，クラウドサービスの価値を高め，ユーザに新しい価値を提供できるようになると考える．

5. あとがき

本稿では，新しいサービス創出に向けて開発したポータブルSIMについて，開発に至った経緯，デバイスの実現手法，基本動作を解説するとともに，新たなサービス創出に向けてポータブルSIMにより拡がる新たな世界についての考えを示した．

今後は，商用化に向けたデバイスの小型化，利便性の向上を図るとともに，ポータブルSIMベースのサービス提供に向けたシステム開発を進めていく予定である．

文　献

[1] Kevin Ashton: “That ‘Internet of Things’ Thing,” RFID Journal, Jun. 2009. http://www.rfidjournal.com/articles/view?4986

[2] Bluetooth SIG, Inc.: “SIM ACCESS PROFILE Interoperability Specification v1.1,” Dec. 2008.

[3] 菅野，ほか：“進化するおサイフケータイ―ドコモUIMカードへのNFC（Type A/B）対応サービス発行の仕組み―，”本誌，Vol.21，No.1，pp.22-28，Apr. 2013.

[4] 秋山，ほか：“進化するおサイフケータイサービスを実現する技術―NFC対応移動機およびドコモUIMカードの開発―，”本誌，Vol.21，No.1，pp.14-21，Apr. 2013.